From checkboxes to frameworks

CISO insights on moving from compliance to risk-based cybersecurity programs

IBM Center for Applied Insights
ibm.com/ibmcai | ibmcai.com

Cybersecurity risk is an immense threat. It’s also a top C-suite priority, with funding for security efforts growing to reflect the gravity of the challenge.

Security leaders are realizing that simply “checking the box” to address compliance requirements is no longer a sufficient strategy. Those further up the maturity curve are transforming their programs to be truly risk-based by using a sophisticated approach to determine risks and prioritize security investments.

Cybersecurity risk is a first-class threat to organizations of all sizes. Managing it is now a top C-suite priority, and funding for security efforts is increasing to reflect its importance. However, the growing number of public breaches occurring despite this increased visibility has led many Chief Information Security Officers (CISOs) and other high-level security leaders to examine their underlying motivations and assumptions. There's a new effort by security leaders to look for fundamental ways to influence and improve both their own programs as well as best practices in effectively defining and applying risk management.

This IBM Center for Applied Insights report, based on "Identifying How Firms Manage Cybersecurity Investment," an IBM-sponsored study by Southern Methodist University, outlines how CISOs are stepping up cybersecurity efforts to focus on addressing one of the most prevalent underlying issues globally—a programmatic focus on compliance instead of risk-based business outcomes.[1] In short, CISOs now know that simply being compliant isn't acceptable for a well-governed organization.

How do I transform a compliance-based security program into one focused on risk?

How can I best communicate risk to the organization and manage expectations?

Do I have the skills, resources and tools to implement the right controls for success?

To address these questions, CISOs are adopting more sophisticated approaches to determine threats and to prioritize and fund security initiatives. Increasingly, security leaders are using custom frameworks as a strategic tool to transform their organizations into ones focused on real cybersecurity risk.

About the study

This IBM Center for Applied Insights report is based on "Identifying How Firms Manage Cybersecurity Investment," an IBM-sponsored study by the Darwin Deason Institute for Cyber Security, part of the Lyle School of Engineering at Southern Methodist University in Dallas, Texas. Researchers surveyed dozens of senior security executives in various industries, with emphasis on financial services, healthcare, retail and government.

In-depth interviews were conducted in a semi-structured approach to explore top cybersecurity risks, how risks are determined, organizational support for cybersecurity initiatives and how investments are prioritized.

About the IBM Center for Applied Insights

ibm.com/ibmcai | ibmcai.com

The IBM Center for Applied Insights introduces new ways of thinking, working and leading. Through evidence-based research, the Center arms leaders with pragmatic guidance and the case for change.

What do CISOs struggle with?

Focusing on the strategic

Historically, cybersecurity investment decisions were commonly based on meeting compliance requirements using best practices and industry-accepted technologies—a “checkbox” approach that satisfied baseline requirements.

Industry best practices were a benchmark for CISOs to gauge whether they had effectively addressed key risk factors for their organizations. If their peers were doing something, it meant they likely should too. And if they were compliant, they could check the box. The challenge for CISOs is that, all too often, a compliance-based approach doesn’t address the actual security risks faced by their organizations.

Communicating priorities

While the majority of senior leaders across organizations realize the importance of cybersecurity, CISOs still need to convey strategy and technical requirements to the C-suite in language they understand.

In addition, CISOs acknowledged that showing ROI for security projects is often difficult—in fact, many firms now view security as a necessary business expense. However, metrics are nonetheless valuable for locking in support for specific initiatives directed by their cybersecurity strategy.

Making cybersecurity strategy consumable

Often, the bigger concern for the C-suite is not whether it should fund cybersecurity initiatives, but whether security teams are equipped to successfully implement controls and manage numerous projects to support the organization.

Part of the challenge is that cybersecurity strategy is not always consumable. Relaying it in a clear implementation plan, selecting the right solutions and developing a deployment schedule that doesn’t disrupt the organization involve a variety of critical factors.

CISOs are struggling to find the right skills to handle the rollout—this requires talent with an exacting mix of technical knowledge and business savvy. Security leaders also have to stay current on market trends, industry best practices and new security product releases.

> *“Good compliance does not equal good security.”*
>
> — CISO, Government

88%

of CISOs reported that their security budgets have increased

CISOs today face three major challenges

Focusing on the strategic

"I always try to make the compliance argument the last thing because I think that way too many programs are aligned around 'What's the minimum thing I have to do to get a check mark?'"

— CISO, Retail

Communicating priorities

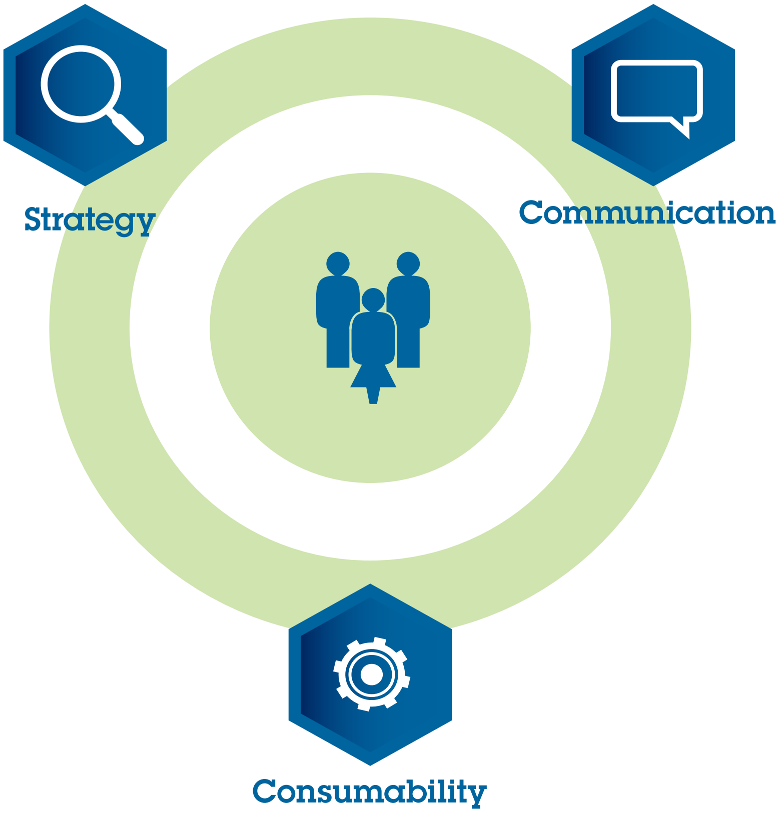
"Senior leadership is looking for me to articulate what the security strategy is in words, in projects, and in dollars that make sense to them."

— CISO, Retail

Making cybersecurity strategy consumable

"It doesn't matter how good the tool is if the program is in the drawer and not on the floor."

— CISO, Financial Services



Using risk-based frameworks to represent and implement cybersecurity strategy

To address the challenges around strategy, communication and implementation, CISOs are increasingly turning to customized frameworks as the primary way to formalize their approach to cybersecurity.

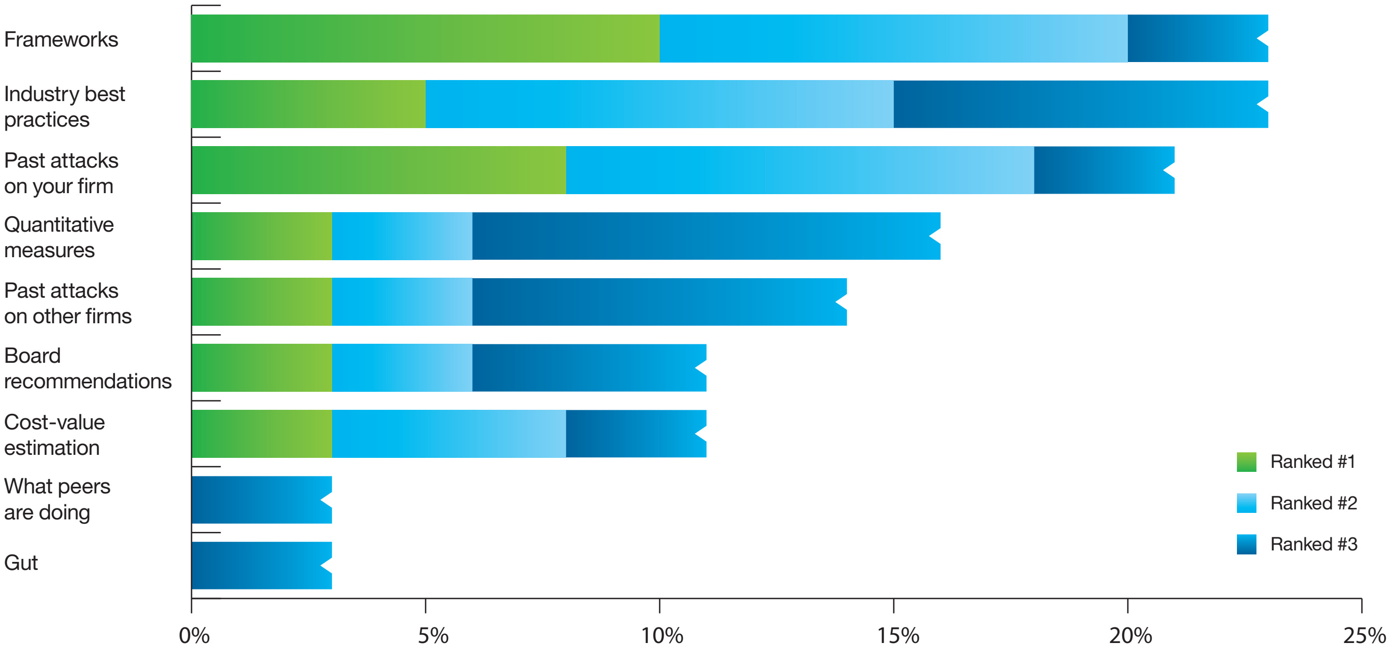
Risk-based frameworks provide standards, best practices and guidelines for protecting systems, applications and data. Frameworks in use range from widely adopted NIST, ISO 2700 and COBIT to hybrid approaches customized for the organization's needs. Frameworks are becoming the strategic tool of choice to assess risk, prioritize threats, secure investment, and communicate progress for the most pressing security initiatives.

Creating effectual policies

A CISO of a financial services firm operates with a clear "three lines of defense" strategy. This means that under the leadership of the COO who has visibility across the organization's operations, the CIO creates policies around risk, or *what* is needed, while the CISO translates those policies into practical implementations, or *how* it will be done. It's the difference between "principle-based" policies that address strategy, and "effectual policies" that address how strategy is implemented.

This approach allows the CISO to create effectual policies, investing in controls that address the real underlying threats to the organization. It also allows investments to be based on customer expectations rather than internal requests. A phased rollout of security controls also helps ensure there are no disruptions to the business and that there's a positive impact on overall security.

Frameworks are ranked as the most strategic prioritization approach



Moving beyond compliance to risk-based strategy

Many of the CISOs interviewed acknowledged that the traditional focus on security compliance allowed them to check a box, but it didn't ensure that the organization was best prepared for potential security breaches.

Frameworks, on the other hand, provide a better risk assessment model, allowing an organization to more thoroughly and consistently assess security challenges and determine gaps. While most frameworks include elements of business assets, processes, vulnerabilities and probabilities, CISOs point to the real value that comes from customizing them based on their environment. This customization mitigates the potential of frameworks to simply become more advanced checkboxes.

Companies developing their own cyber-risk frameworks are more likely to have a deeper understanding of the real risks to their organizations. In most cases, elements of existing frameworks such as NIST and COBIT are used as a foundation to build best-fit frameworks that can be used to inform company-wide standards.

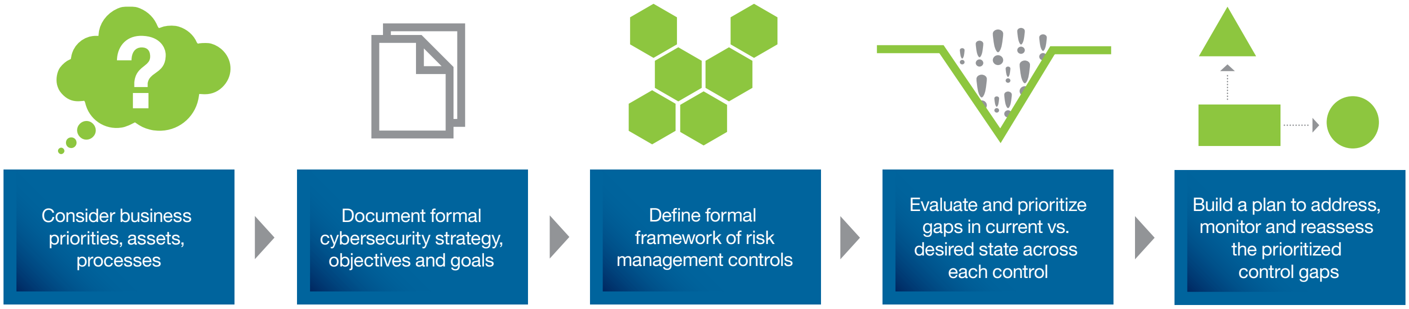
Workbooks for cybersecurity implementation

A VP of security compliance at a data management company takes a different approach that focuses more on assessing cybersecurity risk and less on the actual implementation of cybersecurity strategy. His team develops a project workbook that defines the characteristics of each system to be secured. This workbook provides the approach that is then implemented by the VP of security.

The value of continuous testing is something he stresses: "I don't believe that email, the Internet, anything is secure. Period." Leveraging his background in penetration testing, he continually tests the company's outward-facing applications from an external location, prepared with controls to manage zero-day scenarios. Being nimble allows the security organization to react quickly and protect the company.

> *"Security has to have a basis to argue its point of view in a compelling story with some thought behind it, rather than 'I want to get these things because it's the next cool security thing that's out there.'"*
>
> —CISO, Retail

Strategic cybersecurity programs include five key elements



- Consider business priorities, assets, processes
- Document formal cybersecurity strategy, objectives and goals
- Define formal framework of risk management controls
- Evaluate and prioritize gaps in current vs. desired state across each control
- Build a plan to address, monitor and reassess the prioritized control gaps

Increasing collaboration with the C-suite

Frameworks are also proving to be an effective communication tool, arming CISOs with a translation mechanism to relay cybersecurity strategy to upper management for buy-in. Eighty-five percent of CISOs reported that upper-management support for cybersecurity efforts has increased and 88 percent of CISOs reported that their security budgets have increased.

Nevertheless, when asked about whether they felt that they and peers in other organizations were spending adequately on security initiatives, more than half of the CISOs thought they were spending too little. It's noteworthy that a quarter of the CISOs surveyed who thought they were spending appropriately also used frameworks as a strategic tool.

85%

of CISOs reported that upper-management support for cybersecurity efforts has increased

Orchestrating the lifecycle of cyber defense

A CISO of a financial services firm takes a targeted approach to frameworks in order to address the company's business priorities. Using NIST, ISO and SANS, he developed a customized framework to address the attacks the company was seeing.

The framework focuses on key risks including loss of financial data, financial account compromise, business continuity and regulatory risk. The framework also identified primary threat agents including hacktivists and organized crime.

His team then developed a phased rollout plan to protect against the most common risks using a variety of tools orchestrated to span the full lifecycle of cyber defense, helping ensure business continuity even in the event of a single tool failure. Instead of a peer network of CISOs to guide his investment decisions, this maverick taps the Silicon Valley venture capital community to learn about disruptive new tools that can address his company's security challenges.

> *"It seems like we've all been engaged in a cyber arms race for which we have no option to opt out or seek treaty. There's no other choice but to respond to that threat."*
>
> —CISO, Financial Services

Applying framework-driven cybersecurity insights

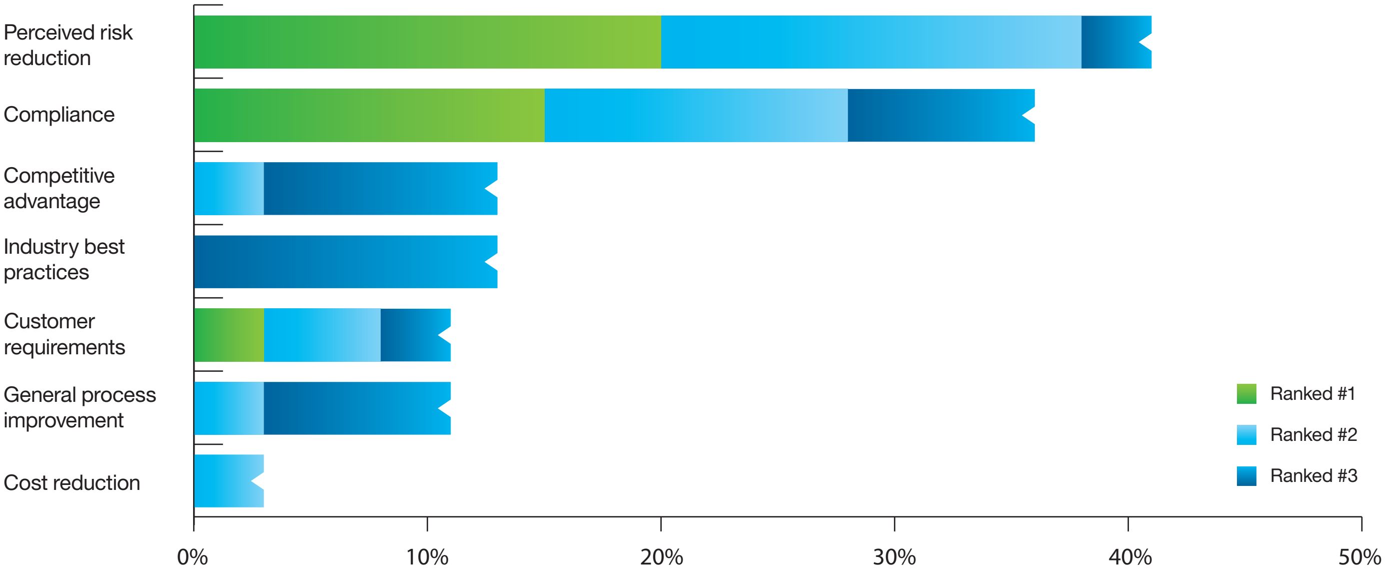
With insights gleaned from new strategic frameworks, what are CISOs prioritizing as drivers for cybersecurity investment? "Perceived risk reduction" and "compliance" still top the list to ensure that baseline security objectives are met. Compliance requirements eat up a significant portion of the security budget. However, perceived risk reduction, evaluated through a framework approach, is helping to drive investment in other security initiatives.

But even when security projects are successfully funded, many CISOs encounter roadblocks to implementation, especially when it comes to finding the right skills. Some CISOs that encountered pushback on budget requests from upper management found that it was because of the concern that the security team wouldn't be able to absorb the approved security spend and execute properly. This talent shortage has led many CISOs to rely on contractors to supplement the skills gap and sometimes even to act in a mentoring capacity to train internal teams.

A recent IBM Center for Applied Insights study, "Shaping security problem solvers: Academic insights to fortify for the future," also highlighted the need to nurture the right security skills to meet the growing needs of organizations.[2] Today's academic security programs are producing versatile experts with technical and business skills who can act as facilitators between IT and the business, bringing predictive and behavioral analysis skills critical to managing cybersecurity programs.

> *"The key is the ability to develop a new skill set where people can adapt to changing environments versus teaching state-of-the-art routines in cybersecurity."*
>
> —Associate Professor of Managed Information Security, United States

Frameworks are helping to drive investments in risk reduction



Whether they are assessing risk, identifying threats or making decisions on the right tools to support their cybersecurity strategy, CISOs overwhelmingly rely on their peer networks as well as third-party information to help inform their decisions. Some CISOs find it valuable to use third-party threat intelligence data feeds to increase visibility to security threats, while others rely on data-loss prevention (DLP) technology. Given these kinds of inputs, 85 percent of CISOs said they had as much information as they needed to select the right security offerings for their organization.

85%

of CISOs reported having the right information to select security solutions for their organization

Raising the bar for cybersecurity strategy

While there's no accounting for the unknown, and all CISOs worry about blind spots, using frameworks as a process enables better preparation, instilling confidence that the right controls are in place and the business is protected. By focusing on custom-building their own frameworks based on industry standards, supplemented by third-party intelligence and input from peer networks, cybersecurity leaders are confronting the actual risks that their organizations face. In addition, frameworks themselves have become a key lens through which to define risk perception at the board level and to prioritize investments in security.

Evolving your cybersecurity program

Move beyond compliance to risk-based strategy
Customize frameworks to enable strategic assessment of the real risks to the organization, highlighting cybersecurity priorities.

Increase collaboration with the C-suite
Use frameworks as an effective communications tool to relay cybersecurity strategy in a more consumable way to stakeholders for buy-in.

Develop
Direct
Deliver

Apply framework-driven cybersecurity insights
Engage the right skills, third-party intelligence and industry best practices to implement the guidance derived from frameworks.

About the authors

Bob Kalka is Vice President of IBM Security, responsible for IBM's global technical sales, strategic accounts and enablement programs. He has held a number of leadership positions in product management, sales, business development, marketing management and product development. Bob is Certified in Risk and Information Systems Control (CRISC) by ISACA, and is ITIL certified. He also holds a US Patent related to secure distributed computing software. Bob can be reached at bkalka@us.ibm.com.

Cynthya Peranandam is Principal Consultant for the IBM Center for Applied Insights, providing data-driven thought leadership to foster strategic conversations. Previously, she led marketing strategy for IBM Social Business solutions and IBM's private cloud platform. Cynthya has worked with clients across the digital spectrum, and has driven adoption and commercialization of emerging technology through IBM's early-adopter program. Cynthya can be reached at cynthya@us.ibm.com and on Twitter @cperanandam. Also check out her posts on the Center's blog.

Contributors

David Jarvis
Caleb Barlow
Sue Ann Wright
Ellen Cornillon

Laura DeLallo
Angie Casey
Walker Harrison

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
October 2015

[1] "Identifying How Firms Manage Cybersecurity Investment," Southern Methodist University, October 2015, http://bit.ly/CISO-cybersecurity-investment

[2] Jarvis, David. *Shaping security problem solvers: Academic insights to fortify for the future*, IBM Center for Applied Insights, 2015, http://bit.ly/academic-insights-on-cybersecurity

The findings described in this report are not to be construed as an endorsement by the Darwin Deason Institute for Cyber Security at SMU. The Darwin Deason Institute for Cyber Security neither agrees nor disagrees with the opinions provided in this report.